IG-98-004

AUDIT REPORT

NASA'S INTEGRATED FINANCIAL MANAGEMENT PROJECT (IFMP) - TIME AND ATTENDANCE/LABOR DISTRIBUTION MODULE

December 17, 1997

National Aeronautics and
Space Administration

OFFICE OF INSPECTOR GENERAL

ADDITIONAL COPIES

To obtain additional copies of this audit report, contact the Acting Assistant Inspector General for Auditing at 202-358-1232

SUGGESTIONS FOR FUTURE AUDITS

To suggest ideas for or to request future audits, contact the Acting Assistant Inspector General for Auditing. Ideas and requests can also be mailed to:

Acting Assistant Inspector General for Auditing
NASA Headquarters
Code W
300 E St., SW
Washington, DC 20546

NASA HOTLINE

To report fraud, waste, abuse, or mismanagement, contact the NASA OIG hotline by calling 1-800-424-9183; 1-800-5358134 (TDD); or by writing the NASA Inspector General, P.O. Box 23089, L'Enfant Plaza Station, Washington, DC 20026. The identity of each writer and caller can be kept confidential upon request to the extent permitted by law.

ACRONYMS

COTS	Commercial Off-the-Shelf Software
EIS	Executive Information System
FLSA	Fair Labor Standards Act
GAO	General Accounting Office
HTTP	Hyper-Text Transfer Protocol
IFMP	Integrated Financial Management Project
JSC	Johnson Space Center
NASA	National Aeronautics and Space Administration
NCSA	National Control and Security Association
NEAT	NASA Employee Attendance Tracking System
NPPS	NASA Personnel and Payroll System
OMB	Office of Management and Budget
RFP	Request for Proposal
SHTTP	Secure Hyper-Text Transfer Protocol
SSL	Secure Socket Layer
T&A	Time and Attendance
WWW	World Wide Web

National Aeronautics and
Space Administration

Headquarters
Washington, DC 20546-0001

Reply to Attn of: W

December 17, 1997

TO: B/IFMP Project Manager

FROM: W/Acting Assistant Inspector General for Auditing

SUBJECT: Final Audit Report
Audit of NASA's IFMP Time and Attendance/Labor Distribution Module
Assignment No. A-HA-97-032
Report No. IG-98-004

We have completed an audit of NASA's IFMP Time and Attendance/Labor Distribution Module. We identified several high risk areas within the process that require management attention in planning appropriate management controls to reduce those risks.

We issued a discussion draft report on October 28, 1997. You provided a written response to the discussion draft on November 25, 1997 in which you concurred with both of our recommendations. We have included the applicable response after each recommendation and the entire response as Appendix 4.

In accordance with NASA Management Instruction 9910.1B, we wish to be included in the concurrence cycle for both recommendations.

If you have any questions or need additional information please call either Lorne A. Dear, Program Director, Infrastructure and Support at (818) 354-3360; Daniel J. Samoviski, Director, Audit Division-A or me at 358-1232.

Robert J. Wesolowski

Enclosure

cc:
B/A. Holz
JM/D. Green
ARC/CFS/A. Sutton

INTRODUCTION

In 1989 NASA was cited by the Office of Management and Budget (OMB) as having a material internal control weakness for not having a standardized, centralized financial accounting system. To correct that problem, NASA, in February 1995, began a new approach to achieve an integrated financial management information system, through the purchase of commercial-off-the-shelf (COTS) software. NASA refers to the project as the Integrated Financial Management Project (IFMP). (Appendix 1 contains a more detailed description of the IFMP development and implementation process.) The Office of Inspector General has been monitoring this project from the beginning and will continue to do so until final implementation. In this capacity, we have been advising management on the development and implementation of the project and have already issued a report and several management letters[1].

BACKGROUND

One of the planned IFMP modules is a time and attendance (T&A)/labor distribution process known as the NASA Employee Attendance Tracking System (NEAT). NEAT complies with recommendations made by the National Performance Review, in that it features exception-based reporting[2] of T&A data. As planned, every NASA employee will have access to NEAT and will be responsible for maintaining their T&A data on electronic time sheets. Electronic routing and approval of T&A data will simplify the traditional attendance certification process by:

- Requiring data entry only if there are exceptions to a pre-established work schedule (e.g., leave, overtime, etc.).
- Eliminating the need for timekeepers and manual record-keeping.

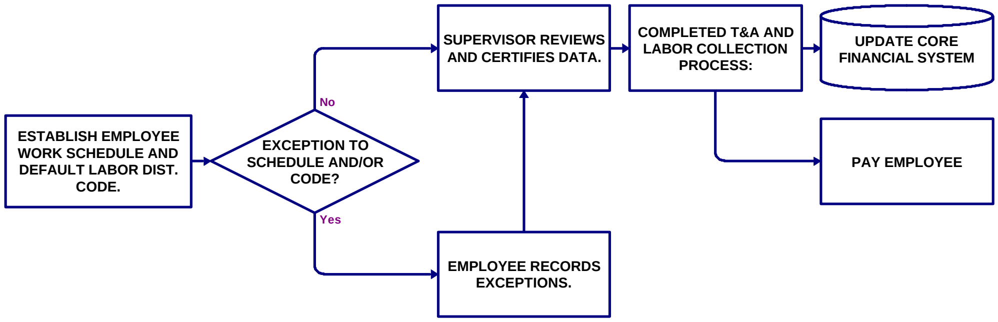
The flowchart on the following page shows the process at a high level:

[1] Other IFMP-related reports issued by the Office of Inspector General:

- Review of the Technical and Procurement Requirements for the Request for Proposal, May 2, 1996. Management Letter number M-HA-96-005.
- Early Phases of NASA's Integrated Financial Management Project, October 21, 1996. Report number IG-97-001.
- Observations Regarding the NASA Employee Attendance Tracking System, July 15, 1997. Management Letter number M-IG-97-011.

[2] Exception-based reporting is a T&A concept where a standard work schedule is established and entered into the system for each employee. The only time the system is updated is when there is an exception to that schedule, such as leave or overtime.

HIGH LEVEL NEAT PROCESS FLOW


ESTABLISH EMPLOYEE WORK SCHEDULE AND DEFAULT LABOR DIST. CODE.
EXCEPTION TO SCHEDULE AND/OR CODE?
No
Yes
SUPERVISOR REVIEWS AND CERTIFIES DATA.
EMPLOYEE RECORDS EXCEPTIONS.
COMPLETED T&A AND LABOR COLLECTION PROCESS:
UPDATE CORE FINANCIAL SYSTEM
PAY EMPLOYEE

As the chart shows, employees only record exceptions to a pre-established work schedule. Timekeepers are not needed.

OBJECTIVE

Our audit objective was to determine whether planned management controls[3] for the NEAT process were adequate.

SCOPE AND METHODOLOGY

The NEAT system requirements that we analyzed were stated at a high level so as not to dictate how the contractor would meet them. The contractor will propose how it will meet those requirements through COTS software. NASA then plans to further refine the process requirements to match the software. Therefore, we intend our recommendations to assist NASA management as it further refines the process requirements.

We performed our audit according to generally accepted government auditing standards. The audit procedures consisted of both a review of the process functional requirements and discussions with project personnel.

[3] Management Control is defined by OMB as: "Organization policies and procedures used by agencies to reasonably ensure that (I) programs achieve their intended results; (ii) resources are used consistent with agency mission; (iii) programs and resources are protected from waste, fraud, and mismanagement; (iv) laws and regulations are followed; and (v) reliable and timely information is obtained, maintained, reported and used for decision making."

AUDIT FIELD WORK

We conducted our fieldwork from March 13 through May 30, 1997 at NASA Headquarters, at several other federal agencies in the Washington, D.C. area, and with the NEAT Process Reengineering Team Leader at JSC.

OVERALL EVALUATION

NASA management has not sufficiently considered necessary management controls for three high-risk areas. The high-risk areas are:

1. Internet access to NEAT.
2. Access to the NASA Personnel and Payroll System.
3. Other NEAT requirements.

We have identified a number of common risks associated with the planned T&A process and some possible controls for mitigating those risks. Those risks and possible controls are listed in Appendix 2. Management plans to develop detailed management controls after they evaluate the contractor's selected COTS software packages. In preparation for that evaluation, the NASA NEAT Process Reengineering Team developed a baseline for a T&A process that will be more efficient. This new process, as designed, has the potential to save NASA time and dollars.

Management Letter

During our audit, we reported several preliminary observations to NASA in a management letter (number M-IG-011, dated July 15, 1997). Specifically, we raised concerns that NASA (1) could possibly save some time and costs by using T&A systems developed by other federal agencies; (2) needs a clearly-defined, documented internal control policy, to include leave without pay (LWOP), overtime, separation of duties, and system reporting; and (3) should consider electronic signature capabilities. In responding to that letter, IFMP management indicated that it had already taken additional steps to improve the planned system by (1) evaluating similar systems in use at other organizations, and (2) initiating a security risk analysis. Based on our continued audit work, we still have some concerns about the planned T&A module. Details follow.

NASA NEEDS TO DEVELOP MANAGEMENT CONTROLS FOR SEVERAL HIGH-RISK AREAS

NASA needs to develop more detailed management controls in the areas of (1) Internet access to NEAT, (2) access to the NASA Personnel and Payroll System and (3) other NEAT requirements. NASA has developed only general, high-level process requirements for the proposed T&A system. Thus, the IFMP and NEAT Teams plan to develop more detailed management control procedures after they: (1) evaluate the contractor- proposed software's capabilities, and (2) complete the final business process reengineering.

OMB Circular A-123, Management Accountability and Control, was revised on June 21, 1995 to assist agencies as they reengineer programs and operations. Section II of the circular requires agencies to take proactive measures to develop cost-effective management controls, as they reengineer their programs and operations.

NASA, should follow the requirements of A-123 and start now in planning reasonable controls to reduce risks. The best first step in planning those controls would be to develop an Internet security policy, and plan a risk management methodology tailored to fit the T&A process. By doing this, NASA will be better prepared to: (1) provide more specific security requirements to both the vendor and the process reengineering teams, and (2) ensure that all necessary controls are implemented timely and cost effectively.

Internet Access to NEAT

Management has not yet addressed specific security requirements for the planned Internet access to the NEAT application. Without adequate Internet security and controls, NEAT will be at greater risk to unauthorized access, hacker[4] attacks, and viruses.

The IFMP Request for Proposal (RFP) requires that IFMP, "employ new and emerging computing and communications technologies that take advantage of open, heterogeneous, distributed architectures."

[4] The term "Hacker" is defined by the General Accounting Office (GAO) as an unauthorized individual who attempts to penetrate information systems; browse, steal, or modify data; deny access or services to others; or cause damage or harm in some other way.

IFMP personnel have expressed their desire to have a world wide web (Web)-based application[5] and have gone as far as to develop a Web-based prototype for NEAT.

The use of the Web creates security risks above and beyond those that exist in traditional T&A systems. Hacker attacks, invasions of privacy, pirating software, and viruses are all more likely to occur in a Web-based application due to the large number of Internet users. (The international accounting firm of Coopers and Lybrand estimates 50 to 55 million Internet users, with a projected increase of one million each month.) Along with the growth of Internet use, the number and skill levels of hackers have also increased. Some studies have shown that in any given year, hackers illegally access US government systems at least 300,000 times through the Internet. According to a recent GAO report, the Department of Defense (DOD) believes that the damage from hacker attacks to DOD systems has cost tens, or possibly hundreds of millions of dollars.

NASA management is aware of the risks associated with Web-based applications and the available security measures. A NASA team issued a draft Information Technology Security Architecture document that addresses network security. The IFMP RFP refers to this document for system security. Also, the NASA Chief Information Officer briefed the IFMP council on Internet security risks and outlined plans for implementing some security mechanisms. During the time of our audit, NASA had not yet finalized and officially released the security document to the public.

The opinion of GAO and at least one large private corporation, regarding Internet security, is that organizations should develop Internet connectivity policies. Those policies should address Internet security, security training, risk analyses, and the application of the various available Internet security mechanisms. (Appendix 3 lists some of the more common Internet security mechanisms.)

[5] Web-based means that the application will be accessed through the Internet by way of the world-wide-web (Web). The Web provides a mechanism for distributing and accessing information across the Internet. The Web model consists of: 1) a *server,* that runs an application on a host computer and sends application information to the Internet; and 2) a *client,* or browser, that runs on the employee/user's desktop and provides an interface to the information on the Internet.

Because every NASA employee will access NEAT from their desktops, employing any of the security mechanisms listed in Appendix 3 could be expensive. (The GAO estimates that firewalls alone can cost between $5,000 and $40,000 for each Internet access point.)

Therefore, we believe that NASA management should develop an overall Internet usage and security policy that includes an assessment of the various security measures in conjunction with identified risks. This will (1) ensure that NASA implements a secure web-based NEAT system in a cost effective manner and (2) help project IFMP budget needs.

Access to the NASA Personnel/Payroll System

One planned functional requirement for NEAT is access to the NASA Personnel/Payroll System (NPPS). According to the RFP, that capability is necessary to retrieve information to support on-line processes, such as retrieval of leave balances. Access to NPPS creates a risk of unauthorized access to NASA personnel and payroll records.

Data on NPPS includes sensitive, Privacy Act related information (such as social security numbers), and other payroll information. Potential access to such data through NEAT introduces additional security risks. Furthermore, having a Web-based T&A system will greatly increase those risks by creating access to that information by the millions of people on the Internet.

The OIG identified several past incidents involving unauthorized access to sensitive information on NPPS. As reported in prior reports, those incidents included:

- A NASA employee who made unauthorized changes to NPPS for personal gain.

- A contractor employee who accessed sensitive data from another employee to harm that employee.

- A former NASA employee who obtained unauthorized data to falsely attest to employment with NASA.

Access to NPPS through NEAT, especially if it is Web-based, increases the risk of such incidents. Management needs to carefully evaluate the need to access NPPS through NEAT, especially if it is Web-based. Alternatively, management will have to consider the cost benefits of various security measures.

Other NEAT Requirements

Management has not planned controls for several other NEAT requirements. Without adequate controls in those areas, NASA could be at risk to unauthorized change to and unauthorized approvals of T&A data.

The NASA requirements for T&A system security, in part, state that the system will have the capability to (1) access and maintain system security at the system level, (2) maintain system security at the application level and (3) maintain system security by function. Before system implementation, NASA needs to consider more detailed security and management control requirements in certain areas where risk is high. Those areas include:

- Adding/modifying exception hours
- Certifying/decertifying data
- Prior pay period adjustments
- Payroll personnel access capabilities
- Fair Labor Standards Act (FLSA) requirements (e.g. overtime payments to FLSA-exempt personnel)

Management should begin now to assess the risks associated with those areas, and plan the management controls necessary to reduce those risks to an acceptable level. If the IFMP contractor's proposed COTS solution does not provide such controls, then necessary compensating controls should be planned. (Additional details on the specific risks and possible controls for each area are in the notes to Appendix 2.)

RECOMMENDATION 1

The IFMP Project Manager should initiate the steps to develop an Internet security policy that documents top management's position on the use of the Web for the T&A module, including management's position on:

- the type of NASA information that should be accessible through the Web.
- NASA's responsibilities for protecting that information.
- the cost effectiveness of Internet security mechanisms.

Management's Response

Concur. The Office of the Chief Financial Officer and the Office of the Chief Information Officer are jointly sponsoring a Computer and Data Security Risk analysis for the IFMP, which is being conducted by Coopers & Lybrand. Among other issues, the analysis will address the protection of certain information as well as the cost of implementing various security measures. The findings will form the basis of the NASA security policy that will be implemented within the IFMP. The estimated completion date is June 1998.

Evaluation of Management's Response

Management's action is responsive to our recommendation. We will keep this recommendation open pending our review of management's final action.

RECOMMENDATION 2

The IFMP Project Manager should initiate the steps to develop a risk management methodology that will ensure that appropriate cost-effective controls are in place to reduce risks to an acceptable level in the following areas:

- Internet access to NEAT.
- Access to the NASA Personnel and Payroll system.
- Modifying exception hours.
- Certifying/decertifying data.
- Prior pay period adjustments.
- Payroll personnel access capabilities.
- FLSA requirements.

Management's Response

Concur. NASA has developed a plan which includes multiple reviews at various levels on the controls to be put in place. All process and policy changes will be reviewed internally within the project, be presented outside the project for review and discussion, and finally presented to the IFMP Council. Also, Coopers and Lybrand, our Independent Verification and Validation agent, will perform an extensive review to determine if adequate security and controls have been incorporated. The overall plan is complete.

Evaluation of Management's Response

Management's action is responsive to our recommendation. We will keep this recommendation open pending our review of management's implementation of its overall quality assurance/management control plan.

IFMP DEVELOPMENT AND IMPLEMENTATION PROCESS

NASA's Chief Financial Officer initiated the Integrated Financial Management Program (IFMP) in February 1995. IFMP's objective is to implement common, agency-wide solutions for many of NASA's business and administrative processes. Several external and internal Agency drivers mandated the establishment of IFMP. Externally, OMB and GAO directed that federal agencies implement financial systems compliant with the JFMIP (Joint Financial Management Information Program, a multi agency cooperative effort to improve government financial management practices). Internal reviews, including NASA's Zero Base Review, also stressed the need to implement a common set of business systems to eliminate non integrated systems and center-unique practices.

NASA's general strategy for implementing IFMP consists of: 1) Reengineering several agency-wide business processes, 2) acquiring commercial-off-the-shelf (COTS) software to meet the process requirements, and 3) implementing full cost accounting.

The project will be broken into two phases. Phase I of the project will focus on six business processes: 1) core financial, 2) budget formulation and execution, 3) procurement, 4) time and attendance, 5) travel, and 6) asset management. Phase II will focus on personnel, payroll, grants, and receivables. An Executive Information System (EIS) will also be established as applications are implemented.

A primary part of IFMP has been to reengineer NASA's processes in order to simplify work flows and reduce overall costs. The teams that NASA established for each business process, have completed most of the reengineering. Their preliminary results are intended to guide the IFMP contractor in selecting and implementing COTS software for each business process. Following the COTS software selections, another period of reengineering will be necessary to identify requirements the COTS software will not support, and to determine how NASA will resolve the differences.

NASA plans to implement IFMP center by center beginning with MSFC by October 1, 1998 and ending with IFMP implemented (Phase I) at all centers by July 1, 1999.

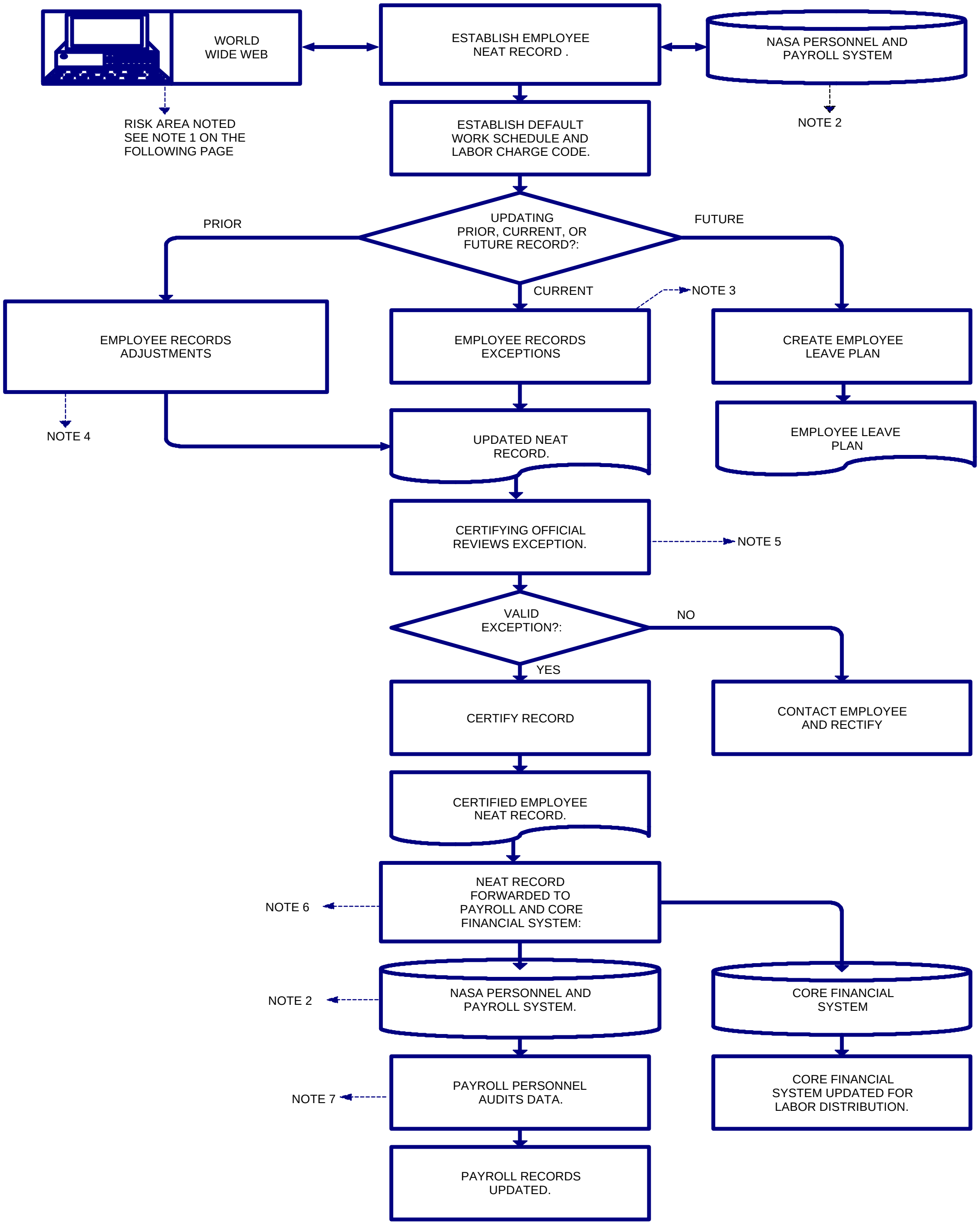
The IFMP Project Manager has emphasized new technology in implementing the project. In September 1995, NASA HQ paid a contractor to develop a prototype for NEAT. The prototype demonstrated new technology that could be used in conjunction with the NEAT application, specifically: 1) the *World Wide Web* as a delivery mechanism to the client, 2) *Java* as an implementation mechanism to distribute some parts of the applications to the client, and 3) an *Expert System* to reduce implementation effort, complexity, and risk.

A large percentage of NASA personnel will use three IFMP processes: time and attendance, travel,

IFMP DEVELOPMENT AND IMPLEMENTATION PROCESS

and procurement. For those three processes management emphasized the new technology as an alternative to installing application software at every employee's workstation. Management believes such technology will substantially reduce software deployment and maintenance costs. NASA purchased an agency wide site license for browser software (Netscape) and made it a standard desk top application.

PROPOSED NEAT PROCESS FLOW AND IDENTIFIED RISKS


WORLD WIDE WEB
ESTABLISH EMPLOYEE NEAT RECORD .
NASA PERSONNEL AND PAYROLL SYSTEM
RISK AREA NOTED SEE NOTE 1 ON THE FOLLOWING PAGE
ESTABLISH DEFAULT WORK SCHEDULE AND LABOR CHARGE CODE.
NOTE 2
PRIOR
UPDATING PRIOR, CURRENT, OR FUTURE RECORD?:
FUTURE
CURRENT
NOTE 3
EMPLOYEE RECORDS ADJUSTMENTS
EMPLOYEE RECORDS EXCEPTIONS
CREATE EMPLOYEE LEAVE PLAN
NOTE 4
UPDATED NEAT RECORD.
EMPLOYEE LEAVE PLAN
CERTIFYING OFFICIAL REVIEWS EXCEPTION.
NOTE 5
VALID EXCEPTION?:
NO
YES
CERTIFY RECORD
CONTACT EMPLOYEE AND RECTIFY
CERTIFIED EMPLOYEE NEAT RECORD.
NOTE 6
NEAT RECORD FORWARDED TO PAYROLL AND CORE FINANCIAL SYSTEM:
NOTE 2
NASA PERSONNEL AND PAYROLL SYSTEM.
CORE FINANCIAL SYSTEM
NOTE 7
PAYROLL PERSONNEL AUDITS DATA.
CORE FINANCIAL SYSTEM UPDATED FOR LABOR DISTRIBUTION.
PAYROLL RECORDS UPDATED.

PROPOSED NEAT PROCESS FLOW AND IDENTIFIED RISKS

NOTES

We developed the following list of risks and possible controls associated with each functional area. This list is based on both our experience in auditing T&A systems as well as the experiences of Inspector General Offices at other agencies. The possible controls are only suggestions for management to consider as they evaluate the likelihood of the risks occurring and the costs of the controls. As emphasized in OMB Circular A-123, implementing those controls are management's responsibility.

Note	*Functional Area*	*Risk(s)*	*Possible Controls*
1	Access to NEAT via World-Wide-Web.	--Unauthorized Access to sensitive data. --Hacker attacks. --Invasions of privacy. --Pirating software --Viruses.	--Clearly documented Internet use security policy. (see Appendix 3 for other possible management controls)
2	Access to the NASA Personnel/Payroll System.	--Unauthorized Access to sensitive data.	--Elimination of this requirement. --Clearly documented policies and procedures. --Access restricted to very few individuals. --Password security. --Logging Procedures
3	Adding/Modifying exception hours.	--Non-accountability of additions/ modifications. --Unauthorized changes.	--Clearly documented policies and procedures. --Access restricted to individual employees own data. --Strict password security.

PROPOSED NEAT PROCESS FLOW AND IDENTIFIED RISKS

NOTES (CONTINUED)

Note	*Functional Area*	*Risk(s)*	*Possible Controls*
4	Prior pay period adjustments.	--Unauthorized changes.	--logging of all adjustments. --supervisory approval and certification of all adjustments.
5	Certify/Decertify/Lock data	--Non-accountability of additions/ modifications. --Unauthorized changes and certifications. --Employees approving their own data.	--Digital signatures. --Clearly documented policies and procedures as to who has certification authority. --Limited Certification authority.
6	FLSA Requirements	--Improper payment of overtime.	--System edits to control payment of overtime to FLSA-exempt employees.
7	Payroll audit capabilities.	--unauthorized access to sensitive NASA data by payroll personnel.	--Restricted access and update capabilities. --Design system to perform this requirement.

APPENDIX 3

DESCRIPTION OF COMMON INTERNET SECURITY MECHANISMS

The following excerpts are taken from a 1997 article in the Auerbach series on Electronic Data Processing Auditing entitled, Auditing Internet Security. The article lists some common Internet security mechanisms and descriptions as follows:

PASSWORD SECURITY AND AUTHENTICATION

Internet security, like personal computer or mainframe security, depends primarily on the use of passwords. The overall security policy should include clearly defined and documented standards for both user names and passwords. With the availability of sophisticated password generation software, passwords should be a combination of alternating upper and lowercase letters mixed with numbers, and not be found in a dictionary. Passwords should be at least six characters long. The longer the password, the more difficult it is to regenerate them by using a program. Names or personal related information that can be ascertained externally should also be avoided. Limitation on the number of password attempts is not standard for the Internet; therefore, Internet-related passwords should be changed more often than internal passwords, at least once per month.

Password protection for disk drives is essential for internally networked personal computers linked to the Internet. Otherwise, external users may be able to access networked personal computer information as a shared resource.

ENCRYPTION OF BUSINESS TRANSACTIONS AND E-MAIL

Encryption is used to avoid information theft during transmission. Encryption software is readily available and two of the most popular products generally work the same. A public and private key encrypts and decrypts messages. Both the sender and receiver have their own private keys, and the sender communicates a public key to the receiver, All software products provide the necessary security for most users, most of the time. As with any encryption routine, experienced cryptographers and hackers can break the algorithm through millions of iterations, if it is worth it to them.

A secure Web browser, such as secure sockets layer (SSL) ensures encryption of all transactions. In addition, instead of using HyperText Transfer Protocol (HTTP), the security protocol, SHTTP, is available. SHTTP, or secure HTTP, encrypts all communication between the browser and the server.

APPENDIX 3

DESCRIPTION OF COMMON INTERNET SECURITY MECHANISMS

FIREWALLS, ROUTERS, AND PROXY SERVERS

A *firewall* is usually a combination of a standalone processor and software, used to deny unauthorized requests for access from the Internet. Firewalls perform comparison of transmission source, file names, and protocols to a predefined table set up by a systems administrator. Firewalls should not be easily disconnected.

A *router* is a hardware device similar to a modem. A router, placed at the front-end of an incoming transmission stream, routes incoming protocols to an appropriate port. Routers restrict access by transmission protocol. Routers should be configured to block access to high risk ports.

A *proxy server* is an application that manages requests to the Internet. Instead of a user communicating directly with the Internet, a user tells the proxy to perform the task. A proxy server is separate from a firewall and adds an additional security layer. Proxies prevent unauthorized uploads and downloads.

WEB SITE SECURITY

Web site links should not access confidential and sensitive information. All transactions should require the use of secured browsers, or secured protocols. Only a Web site administrator and backup personnel should have access to the Web site. Web site server user names and passwords should be kept confidential and changed regularly. Certification of a Web site is necessary whenever sensitive business is transacted. Internet-related organization such as the National Control and Security Association (NCSA) and online service providers are certifying Web sites following a security evaluation.

VIRUS DETECTION

Viruses are common, especially with the availability of freeware and shareware. With the ability of File Transfer Protocol (FTP) across the Web, viruses are even more common. Viruses, among other things, can distort screen messages, corrupt files, and cause screen lockups. To counter those risks, several preventive measures are appropriate. First, avoid loading operating systems from the hard drive. Second, use virus checking software periodically to ensure that dormant viruses are not residing on the hard drive. Third, backup all files from the hard drive.

DESCRIPTION OF COMMON INTERNET SECURITY MECHANISMS

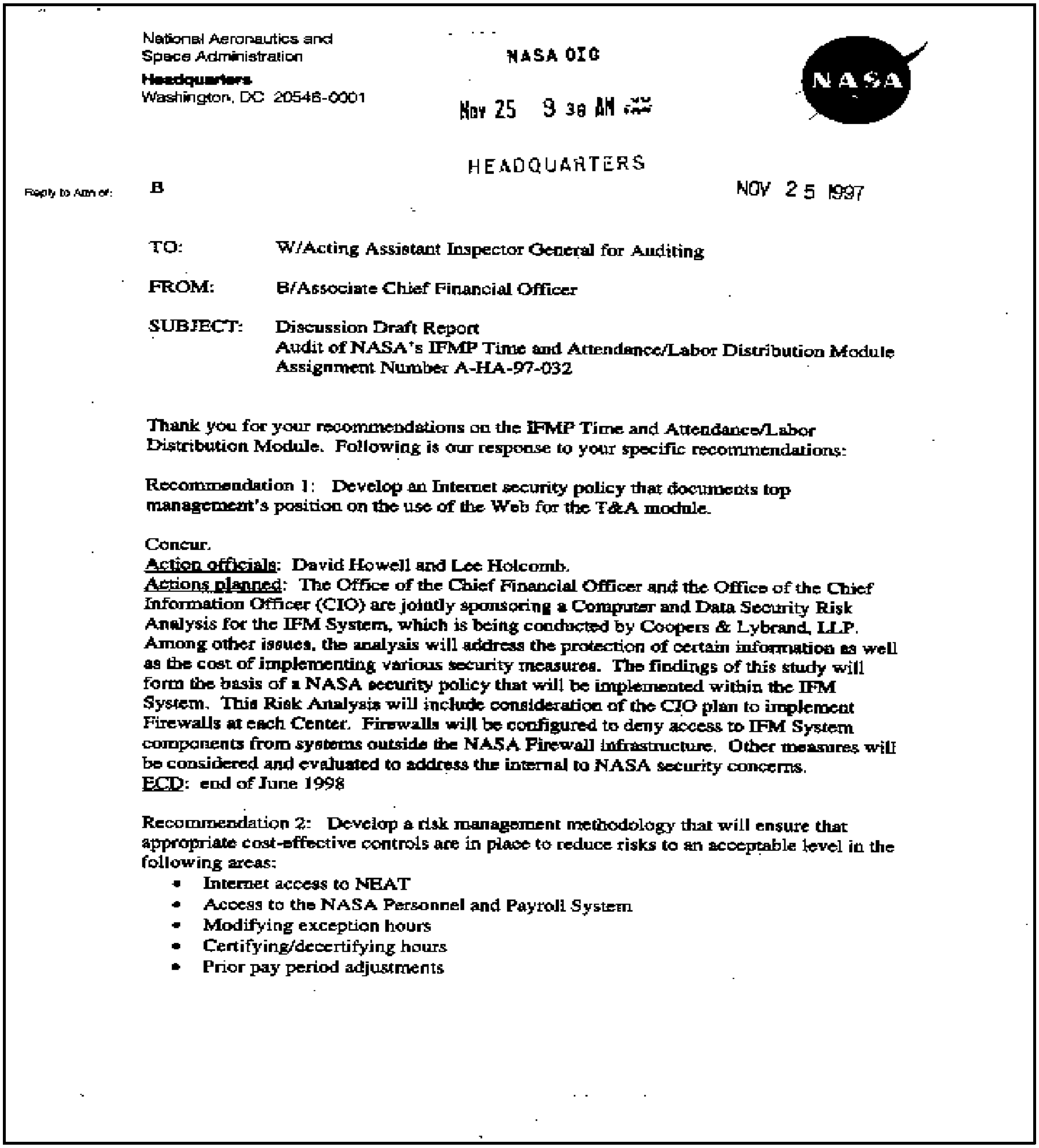
TRANSMISSION LOGGING

All incoming and outgoing transmissions should be logged through firewall, proxy, or other software. A systems or security administrator should review these logs daily. Any unusual trends should be investigated.

PHYSICAL SECURITY AND BACKUPS

Without physical security, circumvention of even the best logical security is possible. A disconnected router, physically bypassed firewall server, or swapped port can sidestep fully implemented logical security. Consequently, physical access restrictions for routers, modems, servers, and telephone lines and ports should be set and included in the overall security policy. For business resumptions in the event of a power outage or disaster, all operating system and network software, along with data backups, should be stored in a secure location, preferably off the site in a location not likely to have suffered from the same disastrous event.

MANAGEMENT'S RESPONSE



National Aeronautics and
Space Administration
Headquarters
Washington, DC 20546-0001

NASA OIG

Nov 25 9 38 AM

HEADQUARTERS

NASA

Reply to Attn of: B

NOV 25 1997

TO: W/Acting Assistant Inspector General for Auditing

FROM: B/Associate Chief Financial Officer

SUBJECT: Discussion Draft Report
Audit of NASA's IFMP Time and Attendance/Labor Distribution Module
Assignment Number A-HA-97-032

Thank you for your recommendations on the IFMP Time and Attendance/Labor Distribution Module. Following is our response to your specific recommendations:

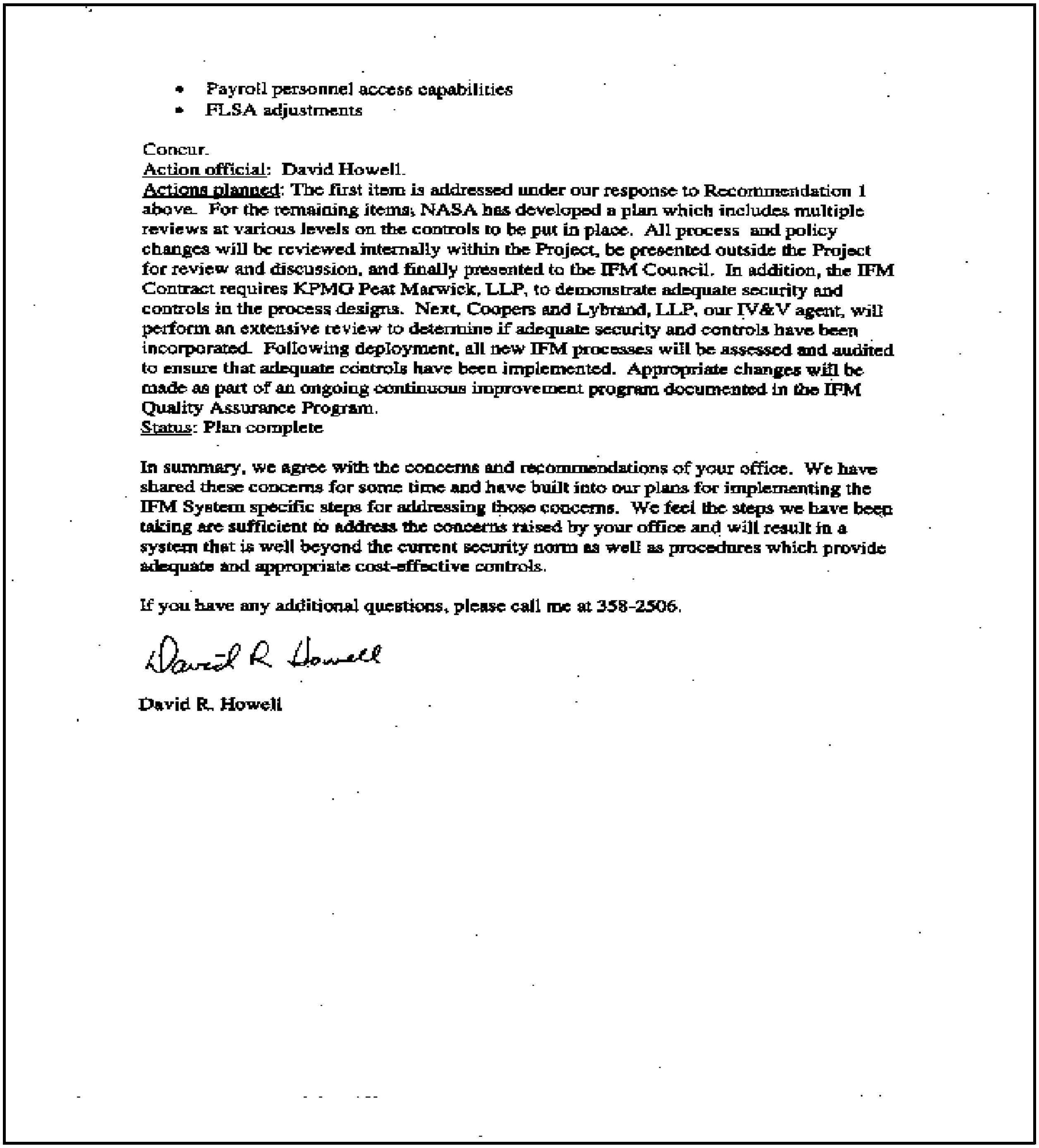
Recommendation 1: Develop an Internet security policy that documents top management's position on the use of the Web for the T&A module.

Concur.
Action officials: David Howell and Lee Holcomb.
Actions planned: The Office of the Chief Financial Officer and the Office of the Chief Information Officer (CIO) are jointly sponsoring a Computer and Data Security Risk Analysis for the IFM System, which is being conducted by Coopers & Lybrand, LLP. Among other issues, the analysis will address the protection of certain information as well as the cost of implementing various security measures. The findings of this study will form the basis of a NASA security policy that will be implemented within the IFM System. This Risk Analysis will include consideration of the CIO plan to implement Firewalls at each Center. Firewalls will be configured to deny access to IFM System components from systems outside the NASA Firewall infrastructure. Other measures will be considered and evaluated to address the internal to NASA security concerns.
ECD: end of June 1998

Recommendation 2: Develop a risk management methodology that will ensure that appropriate cost-effective controls are in place to reduce risks to an acceptable level in the following areas:

- Internet access to NEAT
- Access to the NASA Personnel and Payroll System
- Modifying exception hours
- Certifying/decertifying hours
- Prior pay period adjustments

MANAGEMENT'S RESPONSE



- Payroll personnel access capabilities
- FLSA adjustments

Concur.
Action official: David Howell.
Actions planned: The first item is addressed under our response to Recommendation 1 above. For the remaining items, NASA has developed a plan which includes multiple reviews at various levels on the controls to be put in place. All process and policy changes will be reviewed internally within the Project, be presented outside the Project for review and discussion, and finally presented to the IFM Council. In addition, the IFM Contract requires KPMG Peat Marwick, LLP, to demonstrate adequate security and controls in the process designs. Next, Coopers and Lybrand, LLP, our IV&V agent, will perform an extensive review to determine if adequate security and controls have been incorporated. Following deployment, all new IFM processes will be assessed and audited to ensure that adequate controls have been implemented. Appropriate changes will be made as part of an ongoing continuous improvement program documented in the IFM Quality Assurance Program.
Status: Plan complete

In summary, we agree with the concerns and recommendations of your office. We have shared these concerns for some time and have built into our plans for implementing the IFM System specific steps for addressing those concerns. We feel the steps we have been taking are sufficient to address the concerns raised by your office and will result in a system that is well beyond the current security norm as well as procedures which provide adequate and appropriate cost-effective controls.

If you have any additional questions, please call me at 358-2506.

David R. Howell

David R. Howell

FINAL REPORT DISTRIBUTION

National Aeronautics and Space Administration (NASA) Integrated Financial Management Council Members

Code A/Chief Information Officer
Code B/Deputy Chief Financial Officer
Code B/Deputy Comptroller
Code F/Associate Administrator for Human Resources and Education
Code H/Associate Administrator for Procurement
Code J/Associate Administrator for Management Systems and Facilities
Code Y/Deputy Associate Administrator for Mission to Planet Earth
GSFC-200/Director, Management Operations Directorate, Goddard Space Flight Center

NASA Capital Investment Council Members

Code AT/Associate Deputy Administrator (Technical)
Code G/General Counsel
Code M/Associate Administrator
Code R/Associate Administrator
Code S/R/Associate Administrator
Code U/Associate Administrator
Code Y/Associate Administrator
LaRC/NASA Director
SSC/NASA Director

Other National Aeronautics and Space Administration (NASA) Officials

Code JM/Management Assessment Division (10 copies)
Code L/Associate Administrator For Legislative Affairs

NASA Director, Field Installations

Ames Research Center
Goddard Space Flight Center
Jet Propulsion Laboratory
Lewis Research Center
Marshall Space Flight Center

APPENDIX 5

FINAL REPORT DISTRIBUTION

NASA Offices of Inspector General

Ames Research Center
Goddard Space Flight Center
Jet Propulsion Laboratory
Johnson Space Center
Kennedy Space Center
Langley Research Center
Lewis Research Center
Marshall Space Flight Center

Non-NASA Federal Organizations and Individuals

Assistant to the President for Science and Technology Policy
Deputy Associate Director, Energy and Science Division, Office of Management and Budget
Budget Examiner, Energy Science Division, Office of Management and Budget
Associate Director, National Security and International Affairs Division, General Accounting Office
Special Counsel, Subcommittee on National Security, International Affairs, and Criminal Justice
Professional Assistant, Subcommittee on Science, Technology, and Space, c/o Tom Cooley

Chairman And Ranking Minority Members

Senate Committee on Appropriations
Senate Subcommittee on VA-HUD-Independent Agencies
Senate Committee on Commerce, Science and Transportation
Senate Subcommittee on Science, Technology, and Space
Senate Committee on Governmental Affairs
House Committee on Appropriations
House Subcommittee on VA-HUD-Independent Agencies, Committee on Appropriations
House Committee on Government Reform and Oversight
House Subcommittee on Space and Aeronautics
House Committee on Science

Congressional Members

The Honorable Pete Sessions, U.S. House of Representatives

MAJOR CONTRIBUTORS TO THIS AUDIT

Lorne A. Dear	Program Director, Infrastructure and Support
Karl Allen	Auditor-in-Charge
Tewana Hoskins	Program Assistant